Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 05 July 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The U.S. Customs and Border Protection on Friday announced the launch of a recruiting campaign to hire at least 700 new agents. (See item 9)
- The Washington Post reports that after the Fourth of July celebrations on the Mall, police in Washington, DC, tested the evacuation routes to be used in the event of a terrorist attack. (See item 33)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *July 01, Reuters* — **Rail woes may bring U.S. power summer of discontent.** A long, hot summer combined with railroad disruptions could mean trouble for U.S. coal−burning power plants. With the hottest days of the year ahead and with repairs on the rail track serving coal mines in Wyoming and Montana, some energy industry insiders warn that utilities could run low on fuel as demand for electricity hits its peak. This at a time when many utilities had already let their stocks run down as prices rose, however, some inventories are dangerously low, coal industry experts say. "A continued tight inventory situation and the expected loss of significant Powder River Basin tonnage in the second half of the year should keep the entire coal complex tight," said analyst Jonathan Wolff of Wachovia Capital Markets. Coal industry analyst, Richard Price of Westminster Securities, said utilities that typically had 40 to 60 days

supply now have 20 to 30 days, a level that is sufficient −− barring problems. Much of the problem stems from heavy rain that caused a couple of train derailments in May on the track out of the vast basin. The operators of the line said recently that major track repairs will start in July and last the rest of the year.
Source: http://news.yahoo.com/news?tmpl=story&u=/nm/20050701/lf_nm/bizcoal_power_dc_1

2. *June 30, Reuters* — **OPEC stops talk of more output for now.** Organization of Petroleum Exporting Countries (OPEC) President Sheikh Ahmad al−Fahd al−Sabah said on Thursday, June 30, the cartel had suspended talks on another production increase of 500,000 barrels per day (bpd). This would have been in addition to the 500,000 bpd increase to 28 million bpd for the 10 members of OPEC under quota restrictions that was agreed to this month in Vienna. "There is no shortage of oil in the market," Shiekh Ahmad said. He also said that $53 a barrel was the ideal price for U.S. benchmark crude oil. The OPEC hike of 500,000 agreed June 15 went into effect Friday, July 1. It is near what OPEC has already been actually producing, Sheikh Ahmad said. Sheikh Ahmad, who is also the Kuwaiti oil minister, said the 10 OPEC members under output quotas are currently producing 28.2 million bpd. OPEC produces about 40 percent of the world's oil exports. Sheikh Ahmad said that if OPEC were to agree to increase production again beyond the quota of 28 million bpd, it would lead to an increase of actual production, and not simply a lifting of the quota to agree with real production.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/30/AR2005063001035.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *June 30, Department of Defense* — **Department of Defense releases strategy for homeland defense.** The Department of Defense (DoD) announced on Thursday, June 30, the release of the Strategy for Homeland Defense and Civil Support, a first−ever document that addresses DoD's roles in the homeland defense mission and support to civil authorities. The Strategy for Homeland Defense and Civil Support articulates strategic goals and objectives and provides direction to relevant homeland defense activities across the department. These activities include deterring and preventing attacks, protecting critical defense and designated civilian infrastructure, providing situational understanding, and preparing for and responding to incidents. The strategy focuses on building needed transformational capabilities, enhanced maritime awareness and response capability, strengthened allied contributions to collective security, and improved support to civil authorities.
DoD Strategy for Homeland Defense and Civil Support:
http://www.defenselink.mil/news/Jun2005/d20050630homeland.pdf
Source: http://www.defenselink.mil/releases/2005/nr20050630−3843.html

[Return to top]

Banking and Finance Sector

4. *July 01, Associated Press* — **Banks face challenge in screening employees.** When two of the nation's largest banks were forced to notify thousands of customers that their financial records may have been stolen, there wasn't a hacker, a missing laptop, or a lost box of backup computer tapes to blame. This time, police believe, customers of the banks were the victims of bank employees, workers whose jobs granted them access to valuable information. Security experts believe it's that battle against insiders −− the theft of Social Security numbers and other sensitive data by those with the authority to access it −− that will consume banks and other financial institutions as they fight a recent run of security breaches. Security experts believe inside jobs have the potential to be far more damaging to consumers than accidental losses of data, or attacks by hackers. The protections banks use to thwart hackers have no ability to stop ill−intentioned employees who have authorized access to secure information. Among the steps banks can take to fight insider identity theft is to individually limit each employee's access to customer information, said Avivah Litan, an analyst with IT research firm Gartner. Such a system specifies exactly what customer information each employee can see, touch, and update.
   Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=MF23NLK4E5GKUQSNDBCCKH0CJUMEKJVN?articleID=165600176

5. *June 30, ComputerWorld* — **Credit card data security standard goes into effect.** The Payment Card Industry (PCI) data security standard being pushed by MasterCard International Inc. and Visa U.S.A. Inc. went into effect on Thursday, June 30, for all merchants handling credit card data, but concerns remain about its implementation and compliance validation. Under PCI, all companies that accept credit cards are required to comply with 12 security−related requirements that call for, among other things, encrypted transmission of cardholder data, periodic network scans, logical and physical access controls, activity monitoring and logging. While the PCI standard incorporates sound security practices, there are several issues that still need to be addressed, analysts said. One big shortcoming is that for a majority of the companies, compliance validation is based on self−assessments rather than third−party audits, said Ivan Remsik, an analyst at Cambridge, MA−based Forrester Research Inc. Only the largest merchants −− those processing over six million MasterCard or Visa transactions a year −− are required to submit to formal PCI compliance audits involving formally trained security specialists, Remsik said. As a result, service providers with similar information risk profiles but small differences in transaction volumes are subject to very different compliance requirements, he said.
   PCI data security standard: http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf
   Source: http://www.computerworld.com/printthis/2005/0,4814,102913,00 .html

6. *June 30, Canadian Press* — **E−mails hit record in May as criminals go phishing.** The number of phishing attacks soared to a record high in May, as massive volumes of scam e−mails were sent out by criminals seeking to dupe unsuspecting victims, officials at IBM Corp. said Friday, July 1. IBM officials said that the number of phishing attacks detected in May surpassed the previous record set in January. In May, more than 9.1 million e−mails

containing a phishing scam were detected, more than three times the 2.8 million detected in April and 18 percent higher than the previous record of 7.7 million recorded in January. "We saw a decrease over the past couple of months and then in May we saw a huge increase," said David Mackey, IBM's director of security intelligence. It's unclear who is behind the attacks but they are carried out with software robots, also known as bots −− a program embedded on a computer without the knowledge of its owner and under the control from another site.
Source: http://news.yahoo.com/news?tmpl=story&u=/cpress/20050630/ca_pr_on_tc/ibm_phishing_attacks_2

[Return to top]

Transportation and Border Security Sector

7. *July 01, Department of Transportation* — **Four airports, once used by military, get funds to improve facilities, attract business.** Four airports, all of them once used by the U.S. military, will get federal funds to improve their facilities and attract new business, Department of Transportation Secretary Norman Y. Mineta announced on Friday, July 1. The airports selected today for the Military Airport Program (MAP) are Williams Gateway Airport, Mesa, AZ; Cecil Field, Jacksonville, FL; Guam International Airport, Agana, Guam; and Rickenbacker International Airport, Columbus, OH. MAP is designed to take advantage of the capacity of military airports in order to meet growing demand for air services nationwide. Projects for MAP−designated airports have unique eligibility rules in order to qualify for federal Airport Improvement Program funds to help convert the airports to civilian use. The airports selected have participated previously in the MAP and will receive funds for three years. This year, $34 million will be available through MAP to be divided among the 15 airports, including the four just added, that are participating in the program.
Source: http://www.dot.gov/affairs/dot9405.htm

8. *July 01, Department of Transportation* — **Ohio airports receive $23.2 million to enhance safety and expand capacity.** Airports across Ohio will receive $23.2 million in federal funds to help pay for safety and capacity improvements, U.S. Secretary of Transportation Norman Y. Mineta announced today. The grants to 42 airports will fund a wide range of needs, such as snow removal equipment, new perimeter fencing, and taxiway and terminal improvements. For example, a $7.7 million grant will help Toledo Express Airport upgrade its terminal building and construct a de−icing facility for aircraft, while $3.5 million will be used to open new gates at James M. Cox Airport in Dayton. Runway safety will be improved at Findlay Airport with a $2.3 million grant to extend the taxiway and fund lighting and pavement work.
Source: http://www.dot.gov/affairs/dot9504.htm

9. *July 01, U.S. Customs and Border Protection* — **Border Patrol launches national hiring campaign.** U.S. Customs and Border Protection (CBP) Border Patrol on Friday, July 1, announced the launch of a proactive recruiting campaign in preparation for newly funded positions in FY 2006. Emergency Supplemental Legislation and President Bush's FY06 Budget call for the hiring of an additional 710 agents by the end of FY06. The hiring of these new agents comes in addition to the standard attrition hires that supplement the several hundred agents who retire, transfer, or leave for medical reasons over the course of a year. Currently, nearly 11,000 Border Patrol agents are protecting the more than 6,000 miles of International

Boundary between the official ports of entry with Mexico and Canada, as well mainland coastal waters and the island of Puerto Rico. Border Patrol agents arrested over 1.1 million people last year and seized over 684 tons of illegal narcotics with an estimated value of more than $10.7 billion.
The CBP Border Patrol Hiring Process:
http://www.customs.gov/xp/cgov/careers/customs_careers/border_careers/hiring_process_bp.xml
Source: http://www.customs.gov/xp/cgov/newsroom/press_releases/07012 005.xml

10. *July 01, Department of Transportation* — **Federal funds boost plans to attract business to former Ohio military base.** Rickenbacker International Airport in Columbus, OH, will get federal money to renovate airplane hangars and make other improvements to lure business to the former military base, Department of Transportation Secretary Norman Y. Mineta announced during a visit to the airport on Friday, July 1. The airport is one of several Mineta said would share in funds made available through a program that helps make improvements to former military facilities. According to Mineta, Rickenbacker will receive grants from the Department of Transportation's Military Airport Program for the next three years. The airport will use the grant to renovate three airport hangars into space more appealing to possible tenants. The work includes new and enhanced plumbing, heating, wiring and insulation. This funding will also help build a 48,000 square foot multi−use warehouse that would allow smaller companies to get "in on the action" at Rickenbacker without having to rent an entire hangar, Mineta said.
The Secretary's remarks are available at http://www.dot.gov/affairs/070105MAP.htm.
Source: http://www.dot.gov/affairs/dot9305.htm

11. *July 01, Associated Press* — **Texas homeland security funds planned for border.** The Texas state Homeland Security office says it's sending $5 million to emergency response agencies along the Texas−Mexican border by the end of the year. The funding will be focused on upgrading radio communications. The agencies along the border use different levels of radio frequency technology and equipment, causing communications roadblocks during crises. Laredo will get almost half of the funding −− $2.4 million. Officials say that responds to a higher threat from escalating drug−war violence across the Rio Grande from Laredo in Nuevo Laredo, Mexico.
Source: http://www.news8austin.com/content/headlines/?ArID=140527&Se cID=2

12. *July 01, Associated Press* — **JFK refuelers walk out on Fourth of July weekend.** About 300 airport workers who refuel airplanes at Kennedy International Airport walked out Friday, hours before the start of the Fourth of July holiday weekend that's one of the busiest travel times of the year. The workers' three−year contract expired at midnight Thursday, June 30. The striking members of Teamsters Local 553 were replaced by 130 employees of Allied Aviation Services, a New York−based international company that fuels planes at Kennedy. Allied brought in the replacement workers from Texas, California, Missouri and New Jersey. As of Friday afternoon, July 1, operations at Kennedy appeared to be normal, said Pasquale DiFulco, a spokesperson for the Port Authority of New York and New Jersey, which operates the airport. The last time Local 553 refuelers went on strike at Kennedy was in 1996, and that walkout was settled within 10 days with no major disruption of plane fueling.
Source: http://www.wnbc.com/news/4675822/detail.html

13. *July 01, CNN* — **Report: Flight delays worsening this summer.** Flight delays are worsening this summer, a report by the U.S. Department of Transportation's inspector general has found. In the first half of June, 22 of the nation's major airports had more than a quarter of their flights delayed, according to the survey of airline industry performance released Friday, July 1. At nine airports, the delay rate was more than 30 percent, the survey said. The worst delays were in Atlanta, Georgia, where 35 percent of flights were delayed, it found. Other airports in the Top 10 were Newark, New Jersey; West Palm Beach, Florida; Philadelphia, Pennsylvania; Louisville, Kentucky; Miami, Florida; Fort Lauderdale, Florida; Chicago, Illinois; Washington's Dulles International Airport; and New York's John F. Kennedy International Airport. At those airports, average delays exceeded one hour. But the longest delays −− more than 71 minutes −− occurred at New York's La Guardia Airport. The increasing delays were blamed on soaring demand, along with the growth in low−cost carriers, flight reductions at airline hub airports and a tripling in the use of smaller regional jets, said the report by Inspector General Ken Mead. The report also looked at pricing trends, finding that airfares nationwide have declined since 2000.
Report: AVIATION INDUSTRY PERFORMANCE, http://www.oig.dot.gov/item.jsp?id=1589
Source: http://www.cnn.com/2005/TRAVEL/07/01/flight.delays/index.htm l

14. *June 30, Associated Press* — **Police ram truck to stop car chase at Arizona airport.** Police used patrol cars as battering rams Thursday, June 30, to stop a pickup truck that led officers on a chase that ended at Sky Harbor International Airport in Phoenix, AZ, where controllers were forced to momentarily stop air traffic. The chase began early Thursday in northwest Phoenix as officers responded to a call of a stolen pickup truck, said police spokesperson Sgt. Randy Force. The driver made his way to the airport, where he drove through a security fence, Force said. The truck eventually tore through the fence again, which remained wrapped around the vehicle as police stopped it. Police said the suspect wasn't hit. The man, who identified himself as 29−year−old Damian Holmes of Phoenix, was taken to a hospital for treatment of his injuries before being booked.
Source: http://www.abc15.com/news/index.asp?did=19642

[Return to top]

Postal and Shipping Sector

15. *July 03, Associated Press* — **Lafayette post office receives anthrax detector.** A Lafayette, LA, post office just received a postal service Biohazard Detection System to make anthrax detection in postal mail faster and easier. The Lafayette Central Post Office processes nearly 300 thousand pieces of mail each day. In 2001, it took investigators 14 days to detect anthrax in a piece of mail that went through a New Jersey post office. Postmaster Troy Southerland says the Biohazard Detection System can do it in two hours. The machine is in a secure spot where the mail reaches its first pinch point and collects the air sample at that spot. It uses sterile water and mixes with dust and puts it into a cartridge, where it's identified. When the cartridge is tested, should it turn up active, the light on the top of the machine will go off.
Source: http://www.klfy.com/Global/story.asp?S=3548646

[Return to top]

Agriculture Sector

16. *July 02, Houston Chronicle (TX)* — **Database might help prevent outbreak.** Advocates of a national livestock tracking system say creating a database that identifies every animal and place it has been would speed up future disease investigations but not prevent illnesses. Such a system, already in the works, has been gaining increased attention after the second confirmed case of mad cow disease in the U.S. "The only thing it will prevent is a widespread outbreak," says Amy Spillman, a spokesperson for the U.S. Department of Agriculture's Animal and Plant Health Inspection Service. "We hope to be able to use it to quarantine and eliminate sick animals before a disease gets out of control." Federal regulators developing a three−stage National Animal Identification System want to make participation mandatory by January 2009. Already, 47 states are providing information for the first stage by registering at the state level all locations where livestock are born, raised, fed, housed, exhibited and slaughtered. "We will have all 50 states by the end of July," Spillman said. "And we expect to have cooperative agreements with 25 tribes by the end of the year."
Source: http://www.chron.com/cs/CDA/ssistory.mpl/business/3250398

17. *June 30, All Headline News* — **Fungus found in Kentucky tobacco.** This year's first reported fungus attack on U.S. tobacco plants is coming out of Kentucky. Reportedly, tests revealed blue mold spores on nine acres of a farm near Cecilia, KY, 45 miles southwest of Louisville. University of Kentucky tobacco pathologist Kenny Seebold says, "With that one report, we're very, very concerned that we have it in other places." Mold spores may have been carried by Tropical Storm Arlene, which moved through the area earlier this month. A blue mold outbreak in 1996 cost Kentucky growers an estimated $200 million. Last year, the disease moved quickly through the state and was confirmed in more than 40 counties by July. But, it did not significantly affect the tobacco harvest. Before Seebold's report, the North American Plant Disease Forecast Center had not received any reports of blue mold in the U.S.
Source: http://www.allheadlinenews.com/cgi−bin/news/newsbrief.plx?id =2240315478&fa=1

[Return to top]

Food Sector

18. *July 01, Agence France Presse* — **Mars, Snickers withdrawn from Australian state after contamination threat.** A confectionery manufacturer in Australia pulled Mars Bars and Snickers off its shelves in New South Wales state after a contamination threat. MasterFoods said the two popular chocolate bars were being withdrawn from sale across New South Wales because of the threat by an unknown offender who claimed to have poisoned seven chocolate bars. Detective superintendent Peter Cotter said police were taking the threat seriously after a contaminated chocolate bar was last month sent to confectionery maker MasterFoods, which produces both Snickers and Mars Bars. Cotter said MasterFoods had received three threatening letters from the would−be poisoner, the most recent on Friday, July 1.
Source: http://news.yahoo.com/s/afp/20050701/hl_afp/healthaustraliacrimechocolate_050701105539;_ylt=Al0UMdngTUfXzEsyl_.2hzeJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

19. *July 01, Food and Drug Administration* — **FDA issues alert on Cold Stone Creamery "Cake Batter" ice cream.** The U.S. Food and Drug Administration (FDA) is alerting the public that products containing "cake batter" ice cream sold at Cold Stone Creamery stores throughout the U.S. may be associated with an outbreak of Salmonella Typhimurium infection in several states. After being informed by FDA of the potential contamination problem, Cold Stone Creamery has agreed to immediately remove all "cake batter" ice cream products from its stores throughout the country. "FDA is working with the Centers for Disease Control and Prevention and our state partners to determine the source of the contaminated product and is issuing this alert to protect the public," said Robert Brackett, Director of the FDA's Center for Food Safety and Applied Nutrition." Salmonella Typhimurium is an organism, which can cause serious and sometimes fatal infections in small children, frail or elderly people, and others with weakened immune systems. The ice cream's possible contamination with this organism came to light after multiple cases of infection with this form of Salmonella were reported in late May and early June, 2005 in Minnesota, Washington, Oregon, and Ohio. To date, 14 people are ill from this unusual strain of Salmonella.
Source: http://www.fda.gov/bbs/topics/NEWS/2005/NEW01200.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

20. *July 04, BBC News* — **Scientists hold bird flu summit.** Scientists are meeting in Malaysia to try to find ways to deter a worldwide bird flu epidemic. The conference will focus on protecting farm and market workers and preparing medics and vets for an outbreak. The World Health Organization (WHO) wants a strategy to prevent viruses leaping from animals to humans, and creating a hybrid flu germ. It fears there will almost certainly be a worldwide flu pandemic if action is not taken soon. This meeting brings together delegates from the WHO, the World Organization for Animal Health and the UN's Food and Agriculture Organization. They will focus on high−risk areas like the backyard farms where most of Asia's food is produced and where people and animals live side by side. Other hotspots include wet markets where birds are stored live for shoppers. Experts hope that by encouraging better hygiene and safer working practices it may be possible to stop some animal viruses jumping the species barrier.
Source: http://news.bbc.co.uk/2/hi/asia−pacific/4647485.stm

21. *July 02, Seattle Times (WA)* — **First human case of West Nile virus in Washington state detected.** The Washington state Department of Health confirmed Friday, July 1, that a Spokane−area woman has preliminarily tested positive for the West Nile virus, the first case in a human in Washington state. The case has been labeled as "probable" until further tests are done by the state Public Health Laboratories and the U.S. Centers for Disease Control and Prevention (CDC). It would make Washington the last state in the lower 48 where the virus

spread to humans. CDC results probably will come back in a couple of weeks, Donn Moyer, state health department spokesman, said. He said the local health department in Spokane learned about the woman's "presumptive positive test" from a local laboratory and health−care provider; the local health department then notified the state, he said. It was unclear when each agency learned of the test. The Spokane−area woman, who is in her 20s, had not traveled outside the state before getting sick. She had been briefly hospitalized, he said. In 2002, the virus made its only appearance in Washington −− in four dead birds found in Snohomish, Pend Oreille, Thurston and Pierce counties; and in two horses in Island and Whatcom counties. But the virus didn't get established, probably because not enough birds were infected.
Source: http://seattletimes.nwsource.com/html/localnews/2002355756_h ealthwestnile13.html

22. *July 02, Associated Press* — **Polio found in Angola.** A case of polio has been found in Angola, the first discovered in the country in four years, the World Health Organization (WHO) said Saturday, July 2. "It's a polio case genetically linked to a virus circulating in India," Oliver Rosenbauer, spokesperson for the WHO's polio eradication initiative said. Rosenbauer said the Angolan Ministry of Health contacted WHO in June after a 17−year−old girl developed paralysis in both legs. An investigation has begun to determine how the girl, who lives in the Angolan capital of Luanda, contracted the disease, he said. "The genetic analysis is conclusive," Rosenbauer said. "It is not linked to the cases in the West African outbreak that came from Nigeria and infected Yemen and Indonesia. There's a case investigation going on to see if the family or neighbors have traveled to India," he added.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07 /02/AR2005070200528.html

23. *July 01, Journal of Clinical Investigation* — **Eliminating bacterial infections.** In the days following infection, when the human body develops and refines antibodies and prepares to mount an adaptive immune response, the bulwark of innate host defense against microbial infection is the polymorphonuclear leukocyte (PMN). PMNs seek out, identify, engulf, and sterilize invading microbes using both O2−dependent and O2−independent antimicrobial systems. A decrease in PMN numbers or function caused by immunosuppression or disease increases the risk of infection. Researchers have identified a novel and essential role for hypoxia−inducible factor–1 in regulating several important PMN functions relevant to host defense, including transcription of cationic antimicrobial polypeptides and induction of NO synthase. Hypoxia−inducible factor 1 (HIF−1) is a multisubunit protein that regulates transcription at hypoxia response elements (HREs). By dissecting the role of HIF−1 in innate immune defenses, new targets for therapeutic immunomodulation have been introduced. Several compounds found to activate HIF−1 in vitro have been used in the clinic for other purposes and appear to be well tolerated. These compounds may increase the production of cationic antimicrobial polypeptides through activation of HIF−1 and thereby augment the production of endogenous antibiotics.
Source: http://www.jci.org/cgi/content/full/115/7/1702

[Return to top]

Government Sector

24.

July 01, Associated Press — **Minnesota's Government shuts down.** More than 9,000 state employees were told to stay home Friday, July 1, and drivers found highway rest stops closed at the start of the busy Fourth of July weekend as a budget stalemate led to the first government shutdown in Minnesota history. The Democrats, who control the state Senate, were locked in a standoff with Republican Gov. Tim Pawlenty and the GOP−controlled House over how much to spend on schools and health care and how to pay for it. As a result, the new fiscal year began Friday, just after midnight, with only a partial spending plan in place. Essential services such as the state patrol continued to function, and an 11th−hour agreement was reached to keep state parks open over the holiday weekend. But drivers on one of the busiest travel days of the year found highway rest stops barricaded, and driver's license exam stations and other state offices were closed. Nearly one−fifth of the state workforce was told to stay home and use either vacation time or go without pay.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/01/AR2005070100196.html

25. *June 30, Government Accountability Office* — **GAO−05−526: Immigration Services: Better Contracting Practices Needed at Call Centers (Report).** The U.S. Citizenship and Immigration Services (USCIS) bureau within the Department of Homeland Security (DHS) provides toll−free telephone assistance through call centers to immigrants, their attorneys, and others seeking information about U.S. immigration services and benefits. As the volume of calls increased—from about 13 million calls in fiscal year 2002 to about 21 million calls in fiscal year 2004—questions were raised about USCIS's ability to ensure the reliability and accuracy of the information provided at call centers run by an independent contractor. This report analyzes: (1) the performance measures established by USCIS to monitor and evaluate the performance of contractor operated call centers; (2) how performance measures were used to evaluate the contractor's performance; and (3) any actions USCIS has taken, or plans to take, to strengthen call center operations. To improve USCIS's evaluation of contractor performance, the Government Accountability Office (GAO) recommends that USCIS take steps to ensure that performance measurement provisions are finalized before awarding new contracts and that performance evaluation records are properly maintained. DHS generally agreed with GAO's recommendations and indicated USCIS was taking steps to implement them.
Highlights: http://www.gao.gov/highlights/d05526high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−526

[Return to top]

Emergency Services Sector

26. *July 04, Washington Post* — **Computers simulate terrorism's extremes.** Scientists at the Los Alamos research center in New Mexico have been constructing elaborate computer models of the U.S. to create simulations of a real terrorist attack. There are virtual cities inhabited by millions of virtual individuals. And there are virtual power grids, oil and gas lines, water pipelines, airplane and train systems, even a virtual Internet. When planes crashed into the World Trade Center and Pentagon nearly four years ago, the government had little understanding of the weaknesses and interdependencies of power, water, transportation and telecommunications networks. The models have helped officials pinpoint and prioritize where changes need to be made. The scientists continuously run the simulations, testing actions like

closing the airport, quarantining a neighborhood or shutting down workplaces. Some findings are obvious: that the invention of air transportation may be the biggest factor in the spread of disease. Others aren't as easy to guess: that shutting down schools may not help as much as expected because parents are likely to take their children to malls and playgrounds where they can come in contact with others who have been infected. It also turned out that the speed of intervention is much more important than the type of intervention.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/03/AR2005070300880.html?sub=AR

27. *July 02, East Bay Newspapers (RI)* — **Communities train to respond to oil spill.** Communities from around Buzzards Bay joined together in South Dartmouth, MA, for an all−day drill on Monday, June 27, to prepare them to respond to an oil spill. The Dartmouth location was chosen because Dartmouth received the first of 10 emergency response trailers. The trailers will be loaded with thousands of feet of boom, anchors and an absorbent material that captures oil. They were purchased with funds set aside under the state's Oil Spill Act, enacted in August 2004. The Oil Spill Act created a 2−cent per barrel tax on oil delivered to a marine oil terminal in Massachusetts, including power plants and heating oil company. The trust fund currently contains $1.2 million. The purpose of the Monday's exercise was to keep a simulated oil spill−−comprised of floating oranges, apples and vegetables−−from making its way from Buzzards Bay into the Slocum River. Information about tides and currents was used to plan how to lay out the booms.
Source: http://www.eastbayri.com/story/283659092208019.php

28. *July 01, Hudson Valley News (NY)* — **New York county conducts biohazard drill.** On Thursday, June 30, Orange County, NY, conducted an anthrax drill in the Town of Newburgh, simulating a letter containing the disease being discovered by the Postal Service's Biohazard Detection System. After a simulated response by law enforcement and the county's Hazardous Materials Team, the county Health Department set up a clinic at the Town of Newburgh volunteer Ambulance Corps building to evaluate and provide medication to victims of the simulated bio−terrorism attack. County Health Commissioner Dr. Jean Hudson, who was in charge of the point of distribution clinic for the exercise, emphasized the importance of being able to respond quickly to such an emergency, and to treat people as rapidly as possible.
Source: http://www.midhudsonnews.com/News/OC_biohaz_drill−01Jul05.ht m

29. *June 30, The Wellesley Townsman (MA)* — **Massachusetts towns participate in cross−judisdictional drill.** The health departments of Needham and Wellesley in Massachusetts have a memorandum of understanding to share workforce, services, resources and training across borders. Representatives from Wellesley and Needham's local emergency planning committees (LEPC) have been meeting since January to effectively develop and carry out a drill, testing each town's state of readiness and its ability to respond in an emergency situation. Each agency mobilized its resources to ensure a comprehensive and thoughtful practice. Dr. Paul Biddinger, Associate Director of Science and Technology at the Harvard Center for Emergency Preparedness and a physician at Massachusetts General Hospital, participated in the planning and development meetings, and was the facilitator at the drill. Biddinger developed the scenario, provided props and videos to accompany the written materials and provided the evaluation tool. The drill experience helped showcase the towns' resources and response protocols; served to bring individuals and departments together, so that

they could network and become acquainted in case they hadn't worked together before; and highlighted areas requiring more attention. An after−action report will be used to evaluate the drill and provide guidance for future emergency planning efforts.
Wellesley Emergency Preparedness Website:
http://www.ci.wellesley.ma.us/emergency/index.htm
Wellesley Health Department: http://www.ci.wellesley.ma.us/hth/index.shtml
Source: http://www2.townonline.com/wellesley/localRegional/view.bg?a rticleid=277892

[Return to top]

Information Technology and Telecommunications Sector

30. *July 02, US−CERT* — **Exploit for vulnerability in Microsoft's JVIEW Profiler (javaprxy.dll).** US−CERT is aware of a working public exploit for a vulnerability in the Microsoft JVIEW Profiler (javaprxy.dll) component, an interface to the Microsoft Java Virtual Machine. This vulnerability can be exploited when a user attempts to view an HTML document (e.g., a web page or an HTML email message) that attempts to instantiate the JVIEW Profiler COM object in a certain way. Successful exploitation could allow an attacker to execute arbitrary code on the user's system with privileges of the user. Microsoft has published a Security Advisory about this issue and is continuing to investigate the problem. Until a patch is available to address this vulnerability, US−CERT strongly encourages users to review the workarounds section of Vulnerability Note VU#939605.
VU#939605: http://www.kb.cert.org/vuls/id/939605
Microsoft Security Advisory (903144):
http://www.microsoft.com/technet/security/advisory/903144.ms px
Source: http://www.us−cert.gov/current/current_activity.html#jview

31. *July 01, US−CERT* — **Exploit for vulnerability in phpBB.** US−CERT is aware of a public exploit for a vulnerability in phpBB's "viewtopic.php" script. There are reports of attempts at exploitation, but no confirmed evidence of successful system compromises. A fix for this vulnerability was addressed in version 2.0.11, but did not adequately resolve the issue. In 2004, this vulnerability lead to the propagation of the Santy worm. The phpBB Development Team has released phpBB version 2.0.16 to fully correct this issue. US−CERT encourages administrators to apply the appropriate fixes as soon as possible.
More information about this vulnerability can be found in the following US−CERT Vulnerability Note VU#497400: http://www.kb.cert.org/vuls/id/497400
phpBB version 2.0.16: http://www.phpbb.com/downloads.php
Source: http://www.us−cert.gov/current/current_activity.html#phpBB_v ul

32. *June 30, TechWeb* — **New trojan filtering packets to isolate users.** A new Trojan is using a sophisticated technique to cut off infected computers from anti−virus and security vendors' update sites, the Finnish firm F−Secure said Thursday, June 30. It's not uncommon for worms and Trojan horses to sever links to update sites, but the until recently, said F−Secure, the method has been different: modifying the Windows HOSTS file to redirect the domains of popular security vendors to the local host so that the browser returns a blank page or error. This Trojan, dubbed Fantibag.b by F−Secure (and Fantibag.a by Computer Associates), however, blocks access by creating packet filtering policies using the Microsoft RAS packet filtering

API. The result: all inbound and outbound packets between the user's machine and any of the 100+ filtered IP addresses are then dropped, essentially cutting communication and preventing updates−−such as new malware signatures−−from being downloaded. Among the filtered IP addresses are those belonging to Microsoft (including Windows Update), Computer Associates, F−Secure, McAfee, Sophos, Symantec, and Trend Micro. Fantibag.b sports a tenuous connection with the more prevalent Mitglieder Trojan, said Computer Associates; the former may be downloaded to systems already compromised by Mitglieder.
Source: http://www.techweb.com/wire/security/164904273

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports VERITAS has released security advisories disclosing vulnerabilities that affect multiple versions of Backup Exec for Windows and Netware Servers. Several components of Backup Exec are affected, including the Remote Agent, Server, NetBackup, Web Administration Console, and Admin Plus Pack Option. For more information, please see: http://www.us−cert.gov/current/current_activity.html

The impact of the vulnerabilities ranges from Denial of Service (DoS) conditions to remote execution of arbitrary code. VERITAS has released patches to eliminate all of the reported issues. It is strongly recommended that administrators apply the patches immediately, as historically, vulnerabilities affecting Backup Exec have been targeted by attackers in a widespread fashion:
http://support.veritas.com/menu_ddProduct_BEWNT_view_ALERT.h tm

Updated Port Status: Reports of increased activity on port 6101 have continued. Activity targeting TCP port 10000 has significantly increased since the release of the Metasploit Framework module. Administrators are strongly urged to apply the hotfixes as soon as possible. Strict filtering of TCP port 10000 and 6101 is also highly recommended. For specific hotfixes and udpates please review the following URLs:
http://seer.support.veritas.com/docs/276604.htm
http://www.metasploit.org/projects/Framework/modules/exp loits/backupexec_agent.pm

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 139 (netbios−ssn), 443 (https), 27015 (halflife), 135 (epmap), 1026 (−−−), 53 (domain), 32775 (sometimes−rpc13), 1 (tcpmux), 137 (netbios−ns) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

33. *July 05, Washington Post* — **Evacuation routes tested in nation's capitol after fireworks celebration.** Revelers gathered on the Mall in Washington, DC, to celebrate the Fourth of July, combining the traditional hot dogs, parades and pyrotechnics with a sobering nod to post−September 11 reality: a test of evacuation routes to be used in the event of a terrorist attack. Police set "Operation Fast Forward" into motion at 9:50 p.m., just 15 minutes after the fireworks ended. Over the next 45 minutes, officers directed motorists to four evacuation routes, known as E−routes, where green lights were lengthened from 70 seconds to three minutes, followed by one minute of red. Although the timed lighting appeared to work as planned, a snag resulted from traffic barriers placed by U.S. Park Police to allow pedestrians to leave safely. The barriers created gridlock until they were cleared at 10:10 p.m., with the exercise half over. When the drill ended at 10:35 p.m., lights on a map at the city's command center in the Reeves Municipal Center gradually winked from blue to green. By now, traffic was flowing smoothly throughout the city. An evaluation of the drill will take days or weeks, said Michelle Pourciau, deputy director of the D.C. Department of Transportation.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/04/AR2005070400901.html

[Return to top]

General Sector

34. *July 03, Associated Press* — **Al Qaeda chief of Saudi Arabia killed.** Saudi anti−terror forces killed al Qaeda's top leader in the kingdom in a gunbattle Sunday, July 3, but experts warn the kingdom still faces a surge in attacks despite its two−year crackdown on militants. The 90−minute battle in the eastern Rawdah district, an upscale neighborhood in the capital Riyadh, was the latest blow dealt to al Qaeda in Saudi Arabia, whose leaders have either been killed or captured since authorities launched an unrelenting offensive against it in 2003. Moroccan, Younis Mohammed Ibrahim al−Hayari was killed in a dawn raid by security forces in an area where suspected militants were hiding, an Interior Ministry official was quoted by Saudi Press Agency as saying. Al−Hayari topped a list issued on Tuesday, June 28, of 36 most−wanted militants sought for participation in previous terror attacks in the kingdom dating back to 2003.
Source: http://www.foxnews.com/story/0%2C2933%2C161442%2C00.html

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer